EasyChair Preprint

№ 3485

Employing SABRE Relay Network for Country-Wide Blockchain Network

Aman Pandey and Hakima Chaouchi

May 25, 2020

Employing SABRE relay network for Country-Wide Blockchain network

1st Aman Pandey
Undergraduate Student
National Institute of Technology
Surat, India
aman0902pandey@gmail.com

2nd Hakima Chaouchi
Full Professor
Tèlècom SudParis, Institut Polytechnique de Paris
Paris
hakima.chaouchii@gmail.com

***Abstract*—Internet is taking a turn; services are moving more from centralised to decentralised approach bringing in the revolutions and speeds in the large-industrial applications and energy sector. These sectors are large scale and need a reliable and robust big network for its activities to work. In this paper, we try to support the Public Blockchains as the base for large country-wide networks to carry on its activities. We discuss the SABRE(Secure and Scalable Bitcoin Relay Network), which is a novel relay network designed as a countermeasure of the BGP highjacking attacks on the Bitcoin Network. We see how this method can be generalised for all the Blockchains and how it helps to reach a better network trust. We also discuss that it creates a market place out of block propagation while serving the needs of targetted country-wide Blockchain networks.**

***Index Terms*—public blockchain, relay nodes, routing, security**

I. Introduction

A. Blockchain

Blockchain, which first emerged as the technology behind the cryptocurrencies, resulted in hundreds of other cryptocurrencies, after the successful action of Bitcoin. Blockchain proved to be a concept with Bitcoin, and soon after that emerged as general Decentralised Ledger Technology, with support of the development of dAPPS(Decentralised Applications) on it. Ethereum is currently the most widely spread and successful decentralised application platform, which lets one code smart contracts to leverage its network to run the applications on the Blockchain.

With its success, and promising nature to provide immutable and trustless ledgers, the government across the world has started employing Blockchain, in it is Distribution systems, e.g. Energy Sectors, Water Distribution to factories and other applications. Enterprise has started using it to ensure the safe functioning of the Industrial IoT devices used in its manufacturing plants, to record the IoT status in the Decentralised Ledgers quickly. There have been specific applications in the Country Wide banking network as well. Instead of relying on the central entity, Blockchain leverages the decentralisation and consensus concepts to creating complete and sound systems.

The public or permissionless Blockchains faces scalability, low throughput, the higher rate of orphan blocks and several other issues. Here the permissioned or private Blockchain networks comes into the picture with higher throughput, with less energy consumption, lower orphan block rate, and better scalability. However, the private blockchain brings a certain degree of centralisation by providing authority to several nodes and thus lesser trust in the system, due to controlled privacy and transparency. The data on Private blockchains are prone to censorship. Private Blockchains are good for corporate usage which needs to display different information in different ways, and with certain censorship. There exist specific techniques and implementations to permissions in the public Blockchains.

Identify applicable funding agency here. If none, delete this.

B. Continuous Research and Existing Problems

There had been several systematic pieces of research discussing the challenges associated with the public, private and hybrid blockchains. In Paper [1], several common and specific risks to the blockchain are discussed, which are software-based or basic design based. It also discusses several high level ”real attacks” on the complete Blockchain Systems.

- selfish mining attacks
- DAO Attack
- BGP Highjacking attack
- Eclipse Attack
- Liveness attack
- balance attack

Among these, the BGP(Border Gateway Protocol) highjacking attack is probably the most overlooked until brought into notice with paper [2]. The analysis is done on the Bitcoin system from the networking point of view. The research demonstrates the fact that even after having built over a decentralised network, the Bitcoin network is relatively centralised. The reason is that the majority of the Bitcoin network's mining pool is covered by only a few Autonomous Systems(ASes). Moreover, since the Bitcoin routing is not encrypted, an AS-level adversary can cause dangerous partitioning and delay attacks. The research shows that by highjacking even less than 100 IP prefixes, the Bitcoin network can easily be partitioned, leading into dangerous double chains or delay transaction problems.

The BGP attacks are inevitable, and the protocol is still unstable. Ever since it is known there had already been several

Bitcoin prefix highjacking attacks and probably the network partitioning.

The BGP highjacking attack research was then lead and solved by the introduction of novel relay network technique, SABRE [3], which offers better connection and security to the Bitcoin network at ease to deploy and cost-efficiency of the solution. The SABRE network approach also comes up with several side effects which may prove to be beneficial in case of using Public Blockchains.

C. Outline

In this paper, we will first discuss the available work against the BGP highjacking attacks, and most importantly its solution, which leads to an idea of using SABRE like networks in the regular Public Blockchain designs. Then we will discuss the importance of using Public blockchains for big blockchain networks such as Country vast Government network and what we are precisely doing. We will discuss the benefits SABRE provides to the regular blockchain network and encourage the public blockchain usage for IIoT and Smart Grid networks, based on that. We will discuss the results on the network coverage just by using several Relay nodes, orphan block and the ability to protect the blockchain from the parallel blockchain forks. Following this, we shall discuss the challenges that still prevail and what are the future scopes to support this idea of using SABRE in regular blockchain networks.

II. Related Work

Securing the blockchain against such partitioning attacks is challenging, The portative and short term countermeasures(*as described in* [2]) are not reliable or robust, whereas the internet-wide changes are hard to carry on. Substantial protocol updates are not possible, and will only lead to an increased delay in sending and receiving packets. The problem was discussed for the Bitcoin network and was postulated for other Big networks like Ethereum and Litecoin as well.

Several high-level Blockchain networks like Omniledger[7] tries to solve these problems by freezing commits, but they have to wait for some time before the issue resolves, which makes it unsuitable for our target.

A. Smart Grid and IIoT needs & issues

[9] [10] [11], does some comprehensive study to put Blockchain to practical use for the decentralised energy transfers. [11] proposes a design of Blockchain-based models for ”nearly” real-time monitoring to match supply-demand, as renewable energy generation is not the constant energy sources. Too many peaks and troughs in energy voltage is fatal for grid stability. The proposed models also follow dynamic pricing and incentivisation based on supply-demand. In a countrywide, or possibly the Government's Blockchain-based smart grids could be the target to malicious AS-level adversaries. Small highjacking attacks can lead to a surge in the prevailing rates. Also, it may easily lead to Double spending attacks and Dual Blockchains. Such attacks are not traceable, as the BGP highjacking attacks are still very much uncertain and hidden.

The use of Blockchain in smart energy grids has a direct connection to the use of IoT Devices. For a company, having a countrywide log of its IoT devices, the reliable nodes are necessary, so the SABRE like network designs may help a great deal here.

It turns out that, there is a surge in transforming the Smart Grids to a more Decentralised future. The concept of Energy Internet is recently introduced. It is somehow the necessity to make the system more autonomous. Table II in [12] provides a brief comparison between current and future decentralised smart grids. As in [13], each prosumer needs to install a ETSE(Energy Trading and Security Enhancement) based smart meter, which calculates and broadcasts the energy stats. For permissioned Blockchain it works to interact with the other local smart meter and other ETSE modules. In our case these ETSE modules will be interacting directly with the relay nodes.

Blockchain of Things(BCoT) is taking shape with numerous researches. [14] gives a good systematic study about the needs and perspectives of BCoT. The architecture of BCoT is divided into 5 sub layers: Data, Network, Consensus, Incentive and Service. In the network layer, the IoT devices directly broadcast the message to end servers or cloud services responsible for validation and block mining for you[15]. In this paper we will see how, the relay nodes we are using will act as the end nodes or will be peered directly to the end-servers(which are the end servers provided in an industry).

B. Sabre and what does it do?

SABRE[3] is a secured Bitcoin-specific novel relay network which was designed with the aim to give higher security to Bitcoin clients from getting disconnected from the Bitcoin network and lead to the partitioning of the network.

SABRE is sighted to work with any Blockchain network to implement the *(i) increased security in the block propagation, (ii) providing flexible and partial deployment, (iii) using HW/SW co-design and provide the functionality with very less no of relay nodes, (iv) providing choice in the hands of the client whether they want to connect to the relay node, so that for the higher security and reliability.*

These features make it highly useful for the countrywide networks we are aiming for Blockchains. SABRE aims at providing the relay network which works at the routing-level and provides security to the Block propagation. SABRE uses HW+SW transparent and public design. The relay-nodes are available at the publically announced IP addresses, so any client-node can connect to them. SABRE comes out to be way better than other existing Relay networks when it comes to network-coverage and connection. The SABRE relay nodes receive, validate and transmit the new blocks. The nodes also store the blocks in their cached memory which helps in ignoring the redundant validation and provides quicker propagation. We will discuss the memory required by the Relay nodes and how it is okay to have this amount of configuration. Table

TABLE I
The relay network uses 8 messages.5 exchanged btw switch and controller

Message	**Actions Performed**
GET_SEG	client request particular segment of the block
BLK	actual segment of the block
ADV	client advertises the newly mined blocks
NCONN	switch send to controller to ntoify about new connection
UDP	controller sends it followed by BLK to update the switch memory

TABLE II
THE SWITCH ALSO USES 4 IMPORTANT DATA STRUCTURES

BlockMem	1MB	latest blocks
PeerList	480kB	infomation about connected clients, i.e. who completed 3-way Handshakes
WhiteList	240B	clients that can directly to the controller
BlackList	1.80MB	clients who misused the network, and now are not allowed to connect

II discusses about the memory requirement calculated for the Bitcoin Network.

In Network Design, SABRE, focuses on two checkpoints to be covered, that are required for its reliable implementation, (i) Increasing the no. of nodes that an AS-level attacker may need to highjack in order to do some harmful partition in the network; (ii) increasing the network coverage by the relay network, this makes unlikely for the adversary from stopping clients from getting connected will all the relay nodes.

HW+SW co-design plays an important role. Other than the process of validating and propagating the blocks, they are also required to be reliable and should efficient by compensating the overhead communication required to pass through the relay nodes. This co-design consists of 2 main components a switch & a Controller. The switch is required to serve client connection, protecting controller from the malicious attacks, propagating blocks and storing latest blocks for a faster communication, whereas, the controller in this design is responsible for the validating and communicating the blocks to the connected clients, and last updating the list in the Switch memory.

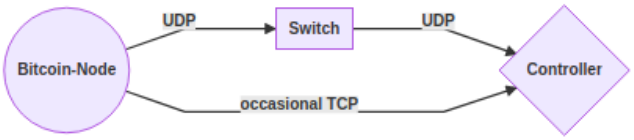
C. Public vs Private

Private Blockchains are generally run by a much smaller and more centralised administrator group, which substantially reduces the cost for the potential attacker to carry out malicious activities, as there are far fewer validator nodes, that can be dominated to take control. The consensus mechanisms may be relatively weaker for the private Blockchains [20]. For the safety reasons sometimes the users in Private Blockchains have to deploy additional resources to ensure network safety.

III. SABRE BASED SECURE ARCHITECTURE PROPOSAL

In this paper we will take the BGP highjacking countermeasure to the Bitcoin network, SABRE and discuss its A. deployability, B. Secure network design C. Transaction flow, with an application perspective in a large Blockchain public network. We will leverage the properties of SABRE network and discuss it's perks in case of such networks.

Fig. 1. Node-Relay Node connection



A. Deployability

The best attribute of the SABRE network is that it is both Fully and Partially deployable. For the complete deployment, the requirements of the SABRE network is *(i) selecting and hosting relay nodes at particular ASes so that it covers a maximum of the network; (ii) using specialised hardware at the locations of the relays.* These relay nodes are then interconnected. The no. of deployed relay nodes decrease the chances that an adversary diverts the traffic. The [3], states about the trade-off between the intra-connectivity between the relay nodes(*e.g. 2-connectivity or k-connectivity*). It tells that as the intra-connectivity increases, it needs more no. of AS level adversaries to disconnect the network but also enables them to disconnect a more significant portion of the network.

It turns out that much of the ASes are the content providers, and they are always trying to increase their connectivity to their peers. So hosting the relay nodes would be more convenient.

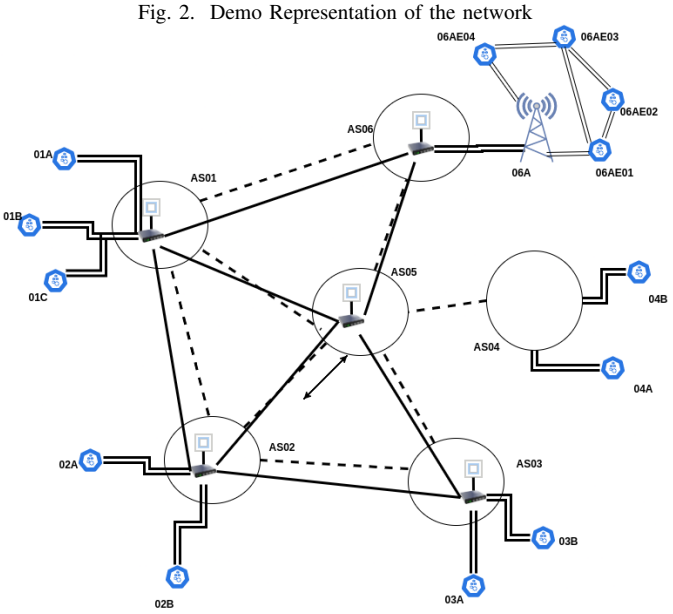
Now there may be some ASes(industries/microgrids) who do not provide consent to host a relay node. In such cases, partial deployment of SABRE nodes can be done. Suppose a mining pool(*a company in case of IIoTs or a regional Smart Grid network*) is willing to protect its network from being partitioned, can deploy the SABRE node in its mining pool. Deploying their own relay nodes secures the block propagation of at least its own blocks, during the attack in the rest of the Blockchain network. This dedicated advantage property would enable large industries to pay for their own good.

B. Creating Secure Network design

The SABRE network [3], has relay-nodes hosted in the /24 prefixes which only belong to ASes which *have no customers, that can peer directly and can form a k-connected graph.* These constructs safe routing for the blocks with the SABRE network employed. These constraints stop the attacker from diverting the relays by advertising more specific prefixes, thus allowing the network to select the authentic advertisements. Plus, the route always happens towards the existing relay nodes(*as the relay nodes always prefer the path of their direct peers rather than any customers*), and thus preventing the attackers from taking advantage by advertising more economically preferred path. Even if the relay nodes find the equally preferred path, it is the one which is directly peered to the ASes hosting the relay nodes. The chances for effective route diversion drops exponentially. Further, the client-node to relay-node connections are protected by hosting the relay nodes on those ASes whose /24 advertisements are more preferred by

ASes with client-nodes. This way, the actions by the malicious ASes can be prevented though it is very much necessary to form an intra-relay network to protect the network from network-level attacks adequately.

Fig. 2. Demo Representation of the network



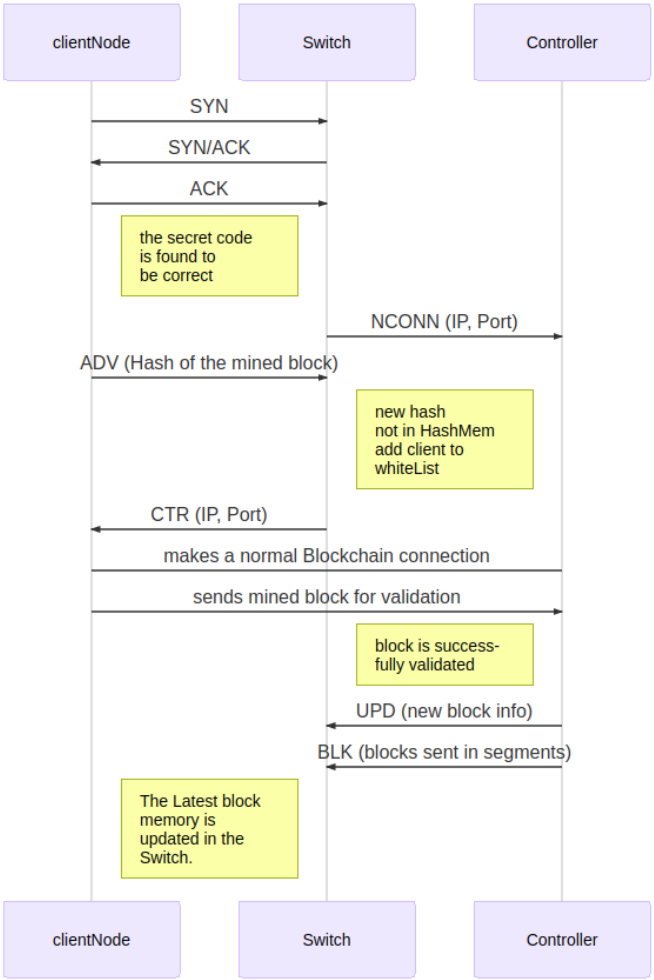
The algorithm in [3] enables to choose the routing path on the basis of following preference customer — peer — provider, shows that, customer AS is preferred over, peer, which in turn is preferred over provider AS.

For the positioning of the relay nodes, a set of ASes that satisfy the above condition are chosen. The chosen ASes must form atleast one k-connected graph of N relay nodes. The ASes which fulfil these criteria that stay intact against most no. of attack models, as well as, has highest network coverage are choosen. See Fig 2. with relay nodes hosted on several ASes. The client nodes connected could be mining pools, micro grids, large enterprise or industry.

C. Transaction

The client nodes initialises its connection with the relay nodes by sending SYN message to the switch of the relay node which is hosted at /24 prefix. The switch reverts with a SYN/ACK message incorporating a secret message with the UDP port. The secret message is acknowledged by the client node to ensure that it is the safe to make connection. The Peerlist is updated with the clients node's IP and a NCONN message is sent to the controller. Whenever a new block is mined, (*which could be a set of transactions, probably log of last 1 hour of IoT devices in the industry*) the client node sends an ADV message containing the HASH of the mined block to the switch. The switch checks if the block is already in its HashMem, if not, the switch sends a CTR message with the (IP, Port) of the controller and adds the client node to its Whitelist. The client node connects to the controller like a normal Blockchain node setting up a UDP connection(*refer Fig 1.*). It is to be noted that a malicious miner cannot overload the controller, as the no. of whitelisted candidate is always kept limited(*it can be regulated acoording to use, and upgrading memory of the relay nodes*). This no. can be set according to the demand of the community, or the hardware capabilities. The whitelisted client nodes are kept in the list for several days(*can be changed*), which allows the relay nodes to know about the "good" pariticipants in the network. If the block is valid the controller updates the switch memory with a new mapping of segment IDs to data segment that corresponds to a particular block hash. The switch can now serve the latest mined blocks independently. (*refer Fig 3.*)

Fig. 3. Transaction Timeline



The newly validated block is now advertised to the rest of the Blockchain network segment by segment like a standard Blockchain advertisement. The other clients can ask for the segments one by one, or the lost one if needed. The switch immediately bans the client that asks for the block multiple times, thus adding it to the *Blacklist*.

D. Incentivising

These relay nodes can later be used for incentivisation programs, where the relay node hosts are getting incentives

to mine and propagate the blocks. [18] discusses providing explicit incentive mechanism for transaction propagation for permissionless blockchains. Incentivising the miners is the only thing encouraging the miners to spend their resources for block mining. Later these incentive mechanism can also be used in case of the large network we are aiming for.

IV. Analysis

The SABRE relay node effectively cover a good amount of network with as low as 6 devices, in case of Bitcoin. Using this system by the government or a nationwide industry certainly provide them with the better security of the Blockchain network they are using, and synchrony between the transactions increases. The relay nodes are k-connected, thus making it more difficult for the attacker to disconnect the relay network (0.5^k for a k-connected node.). However, as already discussed the tradeoff is if the attacker succeeds, it can disconnect a large set of client nodes (*using edge-servers can help*), though it becomes practically challenging.

The safe routing enabled due to intra-connected relay nodes, lead to lesser no. of orphan blocks. The newly configured network is safe from the delay attack, which finally leads to a greater no. of *orphan blocks* or *fork* in the chain. It will at least remain in its normal orphan rate. The normal orphan rate of the Bitcoin network is (*approx* 1%). [16] [17].

The full nodes have to download full blockchain while partial nodes don't. In the case of IIoTs, this point is necessary. The use of SABRE helps in storing the latest block in the switch of the relay nodes and may need to be connected to only a few full nodes. This way, the IIoT devices may get directly connected to the relay nodes, and more beneficially to the controller directly if they are whitelisted.

The network allows ease in forming the community-based network, *e.g. a typical Macro Base Station(MBS) or Small Base station in case of Smart Grids* [14] can be used as end centre which is connected to the SABRE relay node. The general energy business can happen within the community network, and summarised blocks are sent outwards to the relay nodes. In addition to this, the system creates a marketplace to run and host the Relay nodes, and lending them to other small organisations to which the even minute transaction reliability matters.

The IoT devices are more likely to be hacked since their constraints limit the firmware updates. Plus, it is sometimes difficult to carry out software updates on each device in case of Global IoT deployment. Thus, run-time updates and reconfigurations are required to keep IoT devices working securely[21]. The block validation based protocols can then be directly updated to the relay nodes easily by pushing updates to the controller. This way it can be used for updating the firmware to remedy vulnerable breaches, thereby improving the system security. Several initiatives like GITAR[22] and REMOWARE[23], allows the firmware updates in run-time.

The biggest perk of using such a network is implementing standardisation. One national Blockchain running in the backbone of several smaller networks(*community grids, smaller industry*), brings in the national level standardisation. If incorporated by the Government, it will help in running uniform rules across the country and bring in the neutrality.

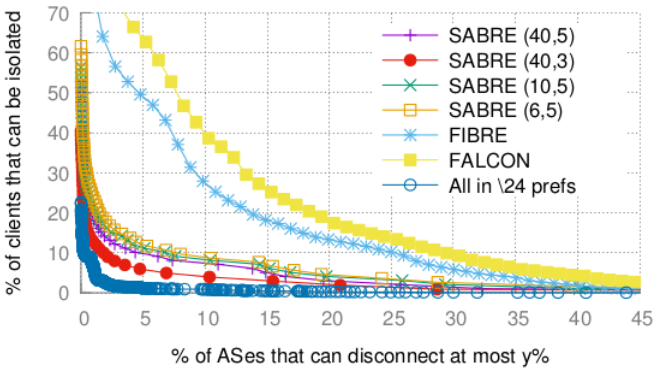
In Fig 2. 06A acts as an MBS which carries its own community which is interconnected using ETSE based client-nodes. Any transaction made among them is piled up and sent at once to the backbone Relay-nodes through 06A or sent one by one, it is configurable and depends upon the usage. 04A and 04B are the nodes connected directly to the ASes, and can still participate in the network. These configurations make the network adjustable and useful for everyone.

V. Challenges

The biggest reason for not using Public Blockchain is still the lower throughput. However this mechanism helps in controlling misuse in the public Blockchain, please note that it does not cause massive improvement in latency. Though, it promises way higher security keeping "at least" previous performance of the network intact. It tries to bring down the throughput issues by providing a mechanism to keep smaller community networks.

Secondly, the k-connected graph is difficult to find; it should be noted that connecting each node is not necessary. Since, there is a trade-off between the connectivity of the relay-nodes and network safety, analysing the optimal point of connectivity is necessary. Citing Fig 4. from [3], we can see that for the BITCOIN network, a 6 single-connected SABRE relay-nodes' deployment can prevent approx 90% of the ASes in the BITCOIN network. Whereas, a 6 node fully-connected network protects only 89.5% of the ASes. The relay-nodes relay among themselves very quickly, so there is no advantage to peering with as many relay nodes as you can find the increased incoming bandwidth during block relay spikes may result in higher latency for your nodes. It reduces the possibility for the partitioning attack by a significant level, but it is still a possibility for an attack.

Fig. 4. "SABRE[3] - Fig 10, for BTC network"



Public networks are transparent, so something to reduce this transparency in case of the public network is necessary. Finally, a standard protocol to make different networks to work together(interoperability) on this network backbone is a necessity.

Another most important thing is the practical and systematic study for such networks. We will try to carry on this research further first with the Blockchain simulation tool SIMBLOCK [4], and then working with actual IoT devices to verify its working and safety while using such networks.

VI. Conclusion

In this paper, we tried to learn about the countermeasure to Bitcoin BGP Highjacking attack by a novel relay network, and it could be used to create a Backbone structure of the large Blockchain networks(*country wide*). We first discussed the available work on Smart Grids & Large IIoT networks as the representatives of the public network we are aiming at, followed by the discussion on the properties of the SABRE network. Then we discussed the partial and full deployability of the SABRE network with comes out to give good advantages in using the network. We then discussed the secure network design of the SABRE network, and that they are hosted on the predefined prefixes. We also discussed the constraints on choosing the ASes to host the relay nodes and how it benefits the Blockchain security. The general Transaction of the network was then discussed, which could be fitted by the standard protocols to make different blockchains work together. The possibility of providing an incentive mechanism was also discussed, which would help to create a marketplace.

The network was then analysed for its safety, and several trade-offs it comes with. The promotion of community Blockchains through this network was also discussed. Further, the challenges and the future scope of research in the field of incentivising the node hosts and creation of standard protocol stated.

References

[1] Li, X., Jiang, P., Chen, T., Luo, X. and Wen, Q., 2020. A Survey On The Security Of Blockchain Systems. [online] arXiv.org. Available at: ¡https://arxiv.org/abs/1802.06993¿ [Accessed 20 April 2020].

[2] M. Apostolaki, A. Zohar and L. Vanbever, "Hijacking Bitcoin: Routing Attacks on Cryptocurrencies," 2017 IEEE Symposium on Security and Privacy (SP), San Jose, CA, 2017, pp. 375-392, doi: 10.1109/SP.2017.29.

[3] Apostolaki, M., Marti, G., Muller, J. and Vanbever, L., 2019. SABRE: Protecting Bitcoin against Routing Attacks. Proceedings 2019 Network and Distributed System Security Symposium,.

[4] Y. Aoki, K. Otsuki, T. Kaneko, R. Banno and K. Shudo, "SimBlock: A Blockchain Network Simulator," IEEE INFOCOM 2019 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), Paris, France, 2019, pp. 325-329, doi: 10.1109/INFCOMW.2019.8845253.

[5] "A Next-Generation Smart Contract and Decentralized Application Platform ," https://github.com/ethereum/wiki/wiki/White-Paper.

[6] Litecoin.org. 2020. Litecoin - Open Source P2P Digital Currency. [online] Available at: ¡https://litecoin.org¿ [Accessed 24 May 2020].

[7] E. Kokoris-Kogias, P. Jovanovic, L. Gasser, N. Gailly, E. Syta and B. Ford, "OmniLedger: A Secure, Scale-Out, Decentralized Ledger via Sharding," 2018 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, 2018, pp. 583-598, doi: 10.1109/SP.2018.000-5.

[8] G. O. Karame, E. Androulaki and S. Capkun, "Double-spending fast payments in bitcoin", _Proc. ACM Conf. Comput. Commun. Secur._, pp. 906-917, 2012.

[9] Z. Li, J. Kang, R. Yu, D. Ye, Q. Deng and Y. Zhang, "Consortium Blockchain for Secure Energy Trading in Industrial Internet of Things," in IEEE Transactions on Industrial Informatics, vol. 14, no. 8, pp. 3690-3700, Aug. 2018, doi: 10.1109/TII.2017.2786307.

[10] N. Z. Aitzhan and D. Svetinovic, "Security and Privacy in Decentralized Energy Trading Through Multi-Signatures, Blockchain and Anonymous Messaging Streams," in IEEE Transactions on Dependable and Secure Computing, vol. 15, no. 5, pp. 840-852, 1 Sept.-Oct. 2018, doi: 10.1109/TDSC.2016.2616861.

[11] C. Pop, T. Cioara, M. Antal, I. Anghel, I. Salomie, and M. Bertoncini, "Blockchain Based Decentralized Management of Demand Response Programs in Smart Energy Grids," _Sensors_, vol. 18, no. 2, p. 162, Jan. 201

[12] Mollah, Muhammad Baqer et al. "Blockchain for Future Smart Grid: A Comprehensive Survey." IEEE Internet of Things Journal (2020): 1–1. Crossref. Web.

[13] F. Lombardi, L. Aniello, S. De Angelis, A. Margheri and V. Sassone, "A blockchain-based infrastructure for reliable and cost-effective IoT-aided smart grids," Living in the Internet of Things: Cybersecurity of the IoT - 2018, London, 2018, pp. 1-6, doi: 10.1049/cp.2018.0042.

[14] H. Dai, Z. Zheng and Y. Zhang, "Blockchain for Internet of Things: A Survey," in IEEE Internet of Things Journal, vol. 6, no. 5, pp. 8076-8094, Oct. 2019, doi: 10.1109/JIOT.2019.2920987.

[15] "Largest Cloud Bitcoin Mining Company — Genesis Mining", Genesis-mining.com. [Online]. Available: https://www.genesis-mining.com/. [Accessed: 22- May- 2020]

[16] C. Decker and R. Wattenhofer, "Information propagation in the bitcoin network," in Peer-to-Peer Computing (P2P), 2013 IEEE Thirteenth International Conference on. IEEE, 2013, pp. 1–10.

[17] M. Imtiaz, D. Starobinski and A. Trachtenberg, "Characterizing Orphan Transactions in the Bitcoin Network", 2019 [Online]. Available: https://arxiv.org/abs/1912.11541. [Accessed: 12- May- 2020]

[18] O. Ersoy, Z. Ren, Z. Erkin, and R. L. Lagendijk. (2017). "Transaction propagation on permissionless blockchains: Incentive and routing mechanisms." [Online]. Available: https://arxiv.org/abs/1712.07564

[19] S. Nakamoto et al., "Bitcoin: A peer-to-peer electronic cash system," 2008.

[20] M. Moos, "Analysis: Bitcoin Costs $1.4 Billion to 51% Attack, Consumes as Much Electricity as Morocco — CryptoSlate", CryptoSlate, 2018. [Online]. Available: https://cryptoslate.com/analysis-bitcoin-costs-1-4-billion-to-51-attack-consumes-as-much-electricity-as-morocco/. [Accessed: 18- May- 2020]

[21] Reyna, A., Martín, C., Chen, J., Soler, E. and Díaz, M., 2018. On blockchain and its integration with IoT. Challenges and opportunities. Future Generation Computer Systems, [online] 88, pp.173-190. Available at: ¡https://doi.org/10.1016/j.future.2018.05.046¿ [Accessed 9 May 2020].

[22] P. Ruckebusch, E. De Poorter, C. Fortuna and I. Moerman, "GITAR: Generic extension for Internet-of-Things ARchitectures enabling dynamic updates of network and application modules", Ad Hoc Networks, vol. 36, pp. 127-151, 2016. Available: 10.1016/j.adhoc.2015.05.017 [Accessed 24 May 2020].

[23] A. Taherkordi, F. Loiret, R. Rouvoy and F. Eliassen, "Optimizing sensor network reprogramming via in situ reconfigurable components", ACM Transactions on Sensor Networks, vol. 9, no. 2, pp. 1-33, 2013. Available: 10.1145/2422966.2422971 [Accessed 24 May 2020].